

(19) 日本国特許庁(JP)

## (12) 公開特許公報(A)

(11) 特許出願公開番号

特開2005-352910

(P2005-352910A)

(43) 公開日 平成17年12月22日(2005.12.22)

(51) Int. Cl.<sup>7</sup>

G06F 15/00

G06F 12/14

F I

G06F 15/00 330A

G06F 12/14 530C

G06F 12/14 530E

テーマコード(参考)

5B017

5B085

審査請求 有 請求項の数 7 O L (全 24 頁)

(21) 出願番号 特願2004-174630 (P2004-174630)

(22) 出願日 平成16年6月11日(2004.6.11)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(74) 代理人 100082131

弁理士 稲本 義雄

(72) 発明者 嶋 久登

東京都品川区北品川6丁目7番35号 ソ

ニー株式会社内

Fターム(参考) 5B017 AA03 BB10 CA16

5B085 AE00

(54) 【発明の名称】 情報処理装置および方法

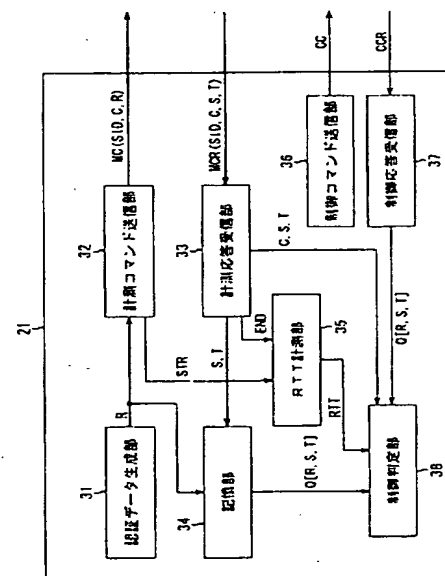
## (57) 【要約】

【課題】例えば著作権で保護されたコンテンツを適切に提供する。

【解決手段】計測コマンド送信部32は、認証データRを含む計測コマンドMCを受信機器に送信する。計測応答受信部33は、送信された計測コマンドMCに対する、受信機器からの応答MCRを受信する。記憶部34は、計測コマンドMCの認証データR、および受信機器からの応答MCRの応答データSと応答生成時間Tを記憶する。RTT計測部35は、往復伝播時間(RTT)を計測する。制御コマンド送信部36は、制御コマンドCCを受信機器に送信する。制御応答受信部37は、制御コマンドCCに対する受信側の機器からの応答CCRを受信する。制御判定部38は、RTTに基づいて、受信機器が同じLAN1内にあるものか否かを判定するとともに、受信機器から正規の機器しか知り得ない情報の提供を受けて、受信機器へのコンテンツの送信を判定する。

【選択図】 図4

図4



## 【特許請求の範囲】

## 【請求項 1】

ネットワークに接続された受信装置に対する所定のコンテンツの送信可否を、所定のコマンドに対する応答にかかる応答時間に基づいて判定する情報処理装置において、

前記受信装置からの、前記コマンドに対する、所定の応答データを含む応答を受信する受信手段と、

前記受信装置からの、前記コマンドに対する応答時間を計測する計測手段と、

前記計測手段により計測された前記応答時間に基づいて、前記受信装置を認証する認証手段と、

前記コマンドに挿入される認証データを生成する生成手段と、

前記生成手段により生成された前記認証データの中の所定のものを含む前記コマンドを、前記認証手段による認証が成功するまで最大  $k$  回、前記受信装置に送信する送信手段と

、前記送信手段により送信された前記コマンドに含まれる前記認証データと、前記受信手段により受信された前記応答に含まれる前記応答データを記憶する記憶手段と、

前記認証手段により認証された前記受信装置に対して、第  $n$  番目に受信された前記コマンドに含まれていた認証データと、その前記コマンドに対する応答に含まれていた応答データの送信を要求する要求手段と、

前記要求手段による要求に応じて、前記受信装置から送信されてきた前記認証データおよび応答データと、第  $n$  番目に送信したコマンドに含まれていた認証データおよびそのコマンドに対する応答に含まれていた応答データとが一致するか否かを判定し、その判定結果に基づいて、前記コンテンツの前記受信装置への送信可否を判定する判定手段と

を備えることを特徴とする情報処理装置。

## 【請求項 2】

前記判定手段は、前記要求手段による要求に応じて、前記受信装置から送信されてきた、前記認証データ、前記応答データ、および前記コンテンツを利用できる装置間で共有する共有データから生成された署名に基づいて、前記受信装置を認証する

ことを特徴とする請求項 1 に記載の情報処理装置。

## 【請求項 3】

前記計測手段は、前記送信手段により前記コマンドが送信されたときから、前記コマンドに対応する応答が前記受信手段により受信されるまでの時間を、前記応答時間として計測する

ことを特徴とする請求項 1 に記載の情報処理装置。

## 【請求項 4】

ネットワークに接続された受信装置に対する所定のコンテンツの送信可否を、所定のコマンドに対する応答にかかる応答時間に基づいて判定する情報処理方法において、

前記受信装置からの、前記コマンドに対する、所定の応答データを含む応答を受信する受信ステップと、

前記受信装置からの、前記コマンドに対する応答時間を計測する計測ステップと、

前記計測ステップの処理で計測された前記応答時間に基づいて、前記受信装置を認証する認証ステップと、

前記コマンドに挿入される認証データを生成する生成ステップと、

前記生成ステップの処理で生成された前記認証データの中の所定のものを含む前記コマンドを、前記認証ステップの処理での認証が成功するまで最大  $k$  回、前記受信装置に送信する送信ステップと、

前記送信ステップの処理で送信された前記コマンドに含まれる前記認証データと、前記受信ステップの処理で受信された前記応答に含まれる前記応答データを記憶する記憶ステップと、

前記認証ステップの処理で認証された前記受信装置に対して、第  $n$  番目に受信された前記コマンドに含まれていた認証データと、その前記コマンドに対する応答に含まれていた

10

20

30

40

50

応答データの送信を要求する要求ステップと、

前記要求ステップの処理での要求に応じて、前記受信装置から送信されてきた前記認証データおよび応答データと、第  $n$  番目に送信したコマンドに含まれていた認証データおよびそのコマンドに対する応答に含まれていた応答データとが一致するか否かを判定し、その判定結果に基づいて、前記コンテンツの前記受信装置への送信可否を判定する判定ステップと

を含むことを特徴とする情報処理方法。

【請求項 5】

ネットワークに接続される送信装置から所定のコンテンツの提供を受ける情報処理装置において、前記送信装置から送信されてきた、所定の認証データを含むコマンドを受信する受信手段と、

前記コマンドに対する、所定の応答データを含む応答を、前記送信装置に送信する第 1 の送信手段と、

前記送信装置からの要求に応じて、第  $n$  番目に受信されてきた前記コマンドに含まれている認証データと、その前記コマンドに対する応答に含まれていた応答データを、前記送信装置に送信する第 2 の送信手段と

を備えることを特徴とする情報処理装置。

【請求項 6】

前記第 2 の送信手段は、前記認証データ、前記応答データ、および前記コンテンツを利用できる装置間で共有する共有データに基づいて署名を生成して、前記送信装置に送信することを特徴とする請求項 5 に記載の情報処理装置。

【請求項 7】

ネットワークに接続される送信装置から所定のコンテンツの提供を受けるための情報処理方法において、

前記送信装置から送信されてきた、所定の認証データを含むコマンドを受信する受信ステップと、

前記コマンドに対する、所定の応答データを含む応答を、前記送信装置に送信する第 1 の送信ステップと、

前記送信装置からの要求に応じて、第  $n$  番目に受信されてきた前記コマンドに含まれている認証データと、その前記コマンドに対する応答に含まれていた応答データを、前記送信装置に送信する第 2 の送信ステップと

を含むことを特徴とする情報処理方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報処理装置および方法に関し、特に、例えば著作権で保護されたコンテンツを適切に授受することができるようにした情報処理装置および方法に関する。

【背景技術】

【0002】

近年、インターネットに代表される公共性のある広域に亘るネットワーク（以下、WAN (Wide Area Network) と称する）や一般家屋等に設けられる局所的なネットワーク（以下、LAN (Local Area Network) と称する）の普及に伴い、それらのネットワークを介した各種データ通信が盛んに行われている。

【0003】

映像や音楽コンテンツなどを、ネットワークを通して伝送する場合は、著作権保護のために、通信相手の機器との間で、認証および鍵交換を行い、コンテンツを暗号化して伝送することが行われている（非特許文献 1 参照）。

【0004】

ここにおいて、著作権の観点からは、家庭内でのコピーや伝送は許可するが、WAN で接続された他の家庭との間でのコンテンツの伝送を制限したい場合がある。例えば、テレビ

10

20

30

40

50

ジョン放送を録画したコンテンツは、私的利用の範囲（家庭内）で利用できるが、インターネットを通して、他人に伝送するのは著作権を侵害すると考えられるので、このような制限が必要となる。

【0005】

この制限の下では、著作権保護されたコンテンツを送信する機器（送信機器）は、そのコンテンツを受信する通信相手の機器（受信機器）が同一LAN内にあるか、WAN（インターネット）を通して接続されているかを判断する必要がある。

【0006】

例えば、IPアドレスから通信相手が同一サブネット内にあるかどうかを調べることや、IP通信パケットが通過したIPルータの数（Hop Count）を使うことで通信相手がWAN（インターネット）を通して接続されているかを知ることができる。しかしながら、WAN（インターネット）を経由した通信であってもVPN（Virtual Private Network）などの技術を使えば、IPルータを経由せずに接続されている同一サブネットであるかのように接続することが可能である。すなわち不正にコンテンツを入手することが可能である。

10

【0007】

そこで、通信相手との間の通信の往復伝播時間（RTT: Round Trip Time）を計測することによって通信距離を判別する方法が提案されている。これはインターネットなどのWANでは、通信距離が長いことおよび、途中のルーターなどの処理にかかる時間などのために、通信データの伝播にかかる時間が家庭内のLANに比べて長くなることを利用するものである。

20

【0008】

例えば図1Aに示すように、送信機器において、受信機器への計測コマンド（S1）の伝送時間、受信機器からの計測コマンドに対する応答（S2）の伝送時間等の往復伝播時間を計測する。同一家庭内のネットワークにおける往復伝播時間は、所定の規定時間（例えば5mS）かそれ以下であるのに比べ、この例のように、インターネット（WAN）を経由した通信は、それ以上（例えば7mS）かかるので、往復伝播時間の長短によって、受信機器がWANを通じて接続されていることを判別することができる。

【0009】

【非特許文献1】DTCP Specification Volume 1 Version 1.3 (Information Version) [http://www.dtcp.com/data/info\\_20040107\\_dtcp\\_Vol\\_1\\_1p3.pdf](http://www.dtcp.com/data/info_20040107_dtcp_Vol_1_1p3.pdf)

30

【発明の開示】

【発明が解決しようとする課題】

【0010】

しかしながら例えば、往復伝播時間だけで、コンテンツの送信可否を判定すると、図1Bに示すように、途中に（例えば同一LANに）第3の機器xを挿入して、計測コマンドに応答することによって、往復伝播時間を短縮することができ、コンテンツを不正に入手することができる。

【0011】

そこで受信機器しか知りえない情報をもって応答させることもできるが、図1Cのように機器xがあらかじめ受信機器に計測コマンド（S21）を送って、受信機器しか知り得ない情報に基づく応答（S22）を取得しておき、送信機器から計測コマンド（S31）が来たときに、覚えておいた応答を返すようにすれば（S32）、正規の機器になりすますことができる。

40

【0012】

本発明は、このような状況に鑑みてなされたものであり、例えば著作権で保護されたコンテンツを適切に授受することができるようにするものである。

【課題を解決するための手段】

【0013】

本発明の第1の情報処理装置は、受信装置からの、コマンドに対する、所定の応答データを含む応答を受信する受信手段と、受信装置からの、コマンドに対する応答時間を計測

50

する計測手段と、計測手段により計測された応答時間に基づいて、受信装置を認証する認証手段と、コマンドに挿入される認証データを生成する生成手段と、生成手段により生成された認証データの中の所定のものを含むコマンドを、認証手段による認証が成功するまで最大  $k$  回、受信装置に送信する送信手段と、送信手段により送信されたコマンドに含まれる認証データと、受信手段により受信された応答に含まれる応答データを記憶する記憶手段と、認証手段により認証された受信装置に対して、第  $n$  番目に受信されたコマンドに含まれていた認証データと、そのコマンドに対する応答に含まれていた応答データの送信を要求する要求手段と、要求手段による要求に応じて、受信装置から送信されてきた認証データおよび応答データと、第  $n$  番目に送信したコマンドに含まれていた認証データおよびそのコマンドに対する応答に含まれていた応答データとが一致するか否かを判定し、その判定結果に基づいて、コンテンツの受信装置への送信可否を判定する判定手段とを備えることを特徴とする。

10

## 【0014】

判定手段は、要求手段による要求に応じて、受信装置から送信されてきた、認証データ、応答データ、およびコンテンツを利用できる装置間で共有する共有データから生成された署名に基づいて、受信装置を認証することができる。

## 【0015】

計測手段は、送信手段によりコマンドが送信されたときから、コマンドに対応する応答が受信手段により受信されるまでの時間を、応答時間として計測することができる。

20

## 【0016】

本発明の第1の情報処理方法は、受信装置からの、コマンドに対する、所定の応答データを含む応答を受信する受信ステップと、受信装置からの、コマンドに対する応答時間を計測する計測ステップと、計測ステップの処理で計測された応答時間に基づいて、受信装置を認証する認証ステップと、コマンドに挿入される認証データを生成する生成ステップと、生成ステップの処理で生成された認証データの中の所定のものを含むコマンドを、認証ステップの処理での認証が成功するまで最大  $k$  回、受信装置に送信する送信ステップと、送信ステップの処理で送信されたコマンドに含まれる認証データと、受信ステップの処理で受信された応答に含まれる応答データを記憶する記憶ステップと、認証ステップの処理で認証された受信装置に対して、第  $n$  番目に受信されたコマンドに含まれていた認証データと、そのコマンドに対する応答に含まれていた応答データの送信を要求する要求ステップと、要求ステップの処理での要求に応じて、受信装置から送信されてきた認証データおよび応答データと、第  $n$  番目に送信したコマンドに含まれていた認証データおよびそのコマンドに対する応答に含まれていた応答データとが一致するか否かを判定し、その判定結果に基づいて、コンテンツの受信装置への送信可否を判定する判定ステップとを含むことを特徴とする。

30

## 【0017】

本発明の第1の情報処理装置および方法においては、受信装置からの、コマンドに対する、所定の応答データを含む応答が受信され、受信装置からの、コマンドに対する応答時間が計測され、計測された応答時間に基づいて、受信装置が認証され、コマンドに挿入される認証データが生成され、生成された認証データの中の所定のものを含むコマンドが、認証が成功するまで最大  $k$  回、受信装置に送信され、送信されたコマンドに含まれる認証データと、受信ステップの処理で受信された応答に含まれる応答データが記憶され、認証された受信装置に対して、第  $n$  番目に受信されたコマンドに含まれていた認証データと、そのコマンドに対する応答に含まれていた応答データの送信が要求され、要求に応じて、受信装置から送信されてきた認証データおよび応答データと、第  $n$  番目に送信したコマンドに含まれていた認証データおよびそのコマンドに対する応答に含まれていた応答データとが一致するか否かが判定され、その判定結果に基づいて、コンテンツの受信装置への送信可否が判定される。

40

## 【0018】

本発明の第2の情報処理装置は、送信装置から送信されてきた、所定の認証データを含

50

むコマンドを受信する受信手段と、コマンドに対する、所定の応答データを含む応答を、送信装置に送信する第1の送信手段と、送信装置からの要求に応じて、第n番目に受信されてきたコマンドに含まれている認証データと、そのコマンドに対する応答に含まれていた応答データを、送信装置に送信する第2の送信手段とを備えることを特徴とする。

【0019】

第2の送信手段は、認証データ、応答データ、およびコンテンツを利用できる装置間で共有する共有データに基づいて署名を生成して、送信装置に送信することができる。

【0020】

本発明の第2の情報処理方法は、送信装置から送信されてきた、所定の認証データを含むコマンドを受信する受信ステップと、コマンドに対する、所定の応答データを含む応答を、送信装置に送信する第1の送信ステップと、送信装置からの要求に応じて、第n番目に受信されてきたコマンドに含まれている認証データと、そのコマンドに対する応答に含まれていた応答データを、送信装置に送信する第2の送信ステップとを含むことを特徴とする。

【0021】

本発明の第2の情報処理装置および方法においては、送信装置から送信されてきた、所定の認証データを含むコマンドが受信され、コマンドに対する、所定の応答データを含む応答が、送信装置に送信され、送信装置からの要求に応じて、第n番目に受信されてきたコマンドに含まれている認証データと、そのコマンドに対する応答に含まれていた応答データが、送信装置に送信される。

【発明の効果】

【0022】

本発明によれば、例えば著作権で保護されたコンテンツを適切に授受することができる。

【発明を実施するための最良の形態】

【0023】

以下に本発明の実施の形態を説明するが、本明細書に記載の発明と、発明の実施の形態との対応関係を例示すると、次のようになる。この記載は、本明細書に記載されている発明をサポートする実施の形態が本明細書に記載されていることを確認するためのものである。従って、発明の実施の形態中には記載されているが、発明に対応するものとして、ここには記載されていない実施の形態があったとしても、そのことは、その実施の形態が、その発明に対応するものではないことを意味するものではない。逆に、実施の形態が発明に対応するものとしてここに記載されていたとしても、そのことは、その実施の形態が、その発明以外の発明には対応しないものであることを意味するものでもない。

【0024】

さらに、この記載は、本明細書に記載されている発明の全てを意味するものではない。換言すれば、この記載は、本明細書に記載されている発明であって、この出願では請求されていない発明の存在、すなわち、将来、分割出願されたり、補正により出現、追加される発明の存在を否定するものではない。

【0025】

本発明の第1の情報処理装置は、受信装置からの、コマンドに対する、所定の応答データを含む応答を受信する受信手段（例えば、図4の計測応答受信部33）と、受信装置からの、コマンドに対する応答時間を計測する計測手段（例えば、図4のRTT計測部35）と、計測手段により計測された応答時間に基づいて、受信装置を認証する認証手段（例えば、図4の制御判定部38）と、コマンドに挿入される認証データを生成する生成手段（例えば、図4の認証データ生成部31）と、生成手段により生成された認証データの中の所定のものを含むコマンドを、認証手段による認証が成功するまで最大k回、受信装置に送信する送信手段（例えば、図4の計測コマンド送信部32）と、送信手段により送信されたコマンドに含まれる認証データと、受信手段により受信された応答に含まれる応答データを記憶する記憶手段（例えば、図4の記憶部34）と、認証手段により認証された受

信装置に対して、第  $n$  番目に受信されたコマンドに含まれていた認証データと、そのコマンドに対する応答に含まれていた応答データの送信を要求する要求手段（例えば、図 4 の制御コマンド送信部 36）と、要求手段による要求に応じて、受信装置から送信されてきた認証データおよび応答データと、第  $n$  番目に送信したコマンドに含まれていた認証データおよびそのコマンドに対する応答に含まれていた応答データとが一致するか否かを判定し、その判定結果に基づいて、コンテンツの受信装置への送信可否を判定する判定手段（例えば、図 4 の制御判定部 38）とを備えることを特徴とする。

#### 【0026】

本発明の第 1 の情報処理方法は、受信装置からの、コマンドに対する、所定の応答データを含む応答を受信する受信ステップ（例えば、図 6 のステップ S 56）と、受信装置からの、コマンドに対する応答時間を計測する計測ステップ（例えば、図 6 のステップ S 55、S 59）と、計測ステップの処理で計測された応答時間に基づいて、受信装置を認証する認証ステップ（例えば、図 6 のステップ S 61）と、コマンドに挿入される認証データを生成する生成ステップ（例えば、図 6 のステップ S 53）と、生成ステップの処理で生成された認証データの中の所定のものを含むコマンドを、認証ステップの処理での認証が成功するまで最大  $k$  回、受信装置に送信する送信ステップ（例えば、図 6 のステップ S 54 乃至ステップ S 63）と、送信ステップの処理で送信されたコマンドに含まれる認証データと、受信ステップの処理で受信された応答に含まれる応答データを記憶する記憶ステップ（例えば、図 6 のステップ S 55、S 60）と、認証ステップの処理で認証された受信装置に対して、第  $n$  番目に受信されたコマンドに含まれていた認証データと、そのコマンドに対する応答に含まれていた応答データの送信を要求する要求ステップ（例えば、図 6 のステップ S 64）と、要求ステップの処理での要求に応じて、受信装置から送信されてきた認証データおよび応答データと、第  $n$  番目に送信したコマンドに含まれていた認証データおよびそのコマンドに対する応答に含まれていた応答データとが一致するか否かを判定し、その判定結果に基づいて、コンテンツの受信装置への送信可否を判定する判定ステップ（例えば、図 6 のステップ S 66）とを含むことを特徴とする。

#### 【0027】

本発明の第 2 の情報処理装置は、送信装置から送信されてきた、所定の認証データを含むコマンドを受信する受信手段（例えば、図 5 の計測コマンド受信部 53）と、コマンドに対する、所定の応答データを含む応答を、送信装置に送信する第 1 の送信手段（例えば、図 5 の計測応答送信部 55）と、送信装置からの要求に応じて、第  $n$  番目に受信されてきたコマンドに含まれている認証データと、そのコマンドに対する応答に含まれていた応答データを、送信装置に送信する第 2 の送信手段（例えば、図 5 の制御応答送信部 58）とを備えることを特徴とする。

#### 【0028】

本発明の第 2 の情報処理方法は、送信装置から送信されてきた、所定の認証データを含むコマンドを受信する受信ステップ（例えば、図 7 のステップ S 86）と、コマンドに対する、所定の応答データを含む応答を、送信装置に送信する第 1 の送信ステップ（例えば、図 7 のステップ S 92）と、送信装置からの要求に応じて、第  $n$  番目に受信されてきたコマンドに含まれている認証データと、そのコマンドに対する応答に含まれていた応答データを、送信装置に送信する第 2 の送信ステップ（例えば、図 7 のステップ S 94）とを含むことを特徴とする。

#### 【0029】

図 2 は、本発明を適用した端末 11 からなる通信システムの構成例を示している。

#### 【0030】

LAN1-1、1-2（以下、個々に区別する必要がない場合、単に、LAN1 と称する。他の場合についても同様である）がインターネットに代表される WAN2 を介して相互に接続されている。

#### 【0031】

LAN1-1 は、例えば、家屋内に設けられ、特定の個人（あるいは、家族）が使用する

程度の規模のものであり、それには、スイッチングハブ（図示せず）を介して、パーソナルコンピュータやAV機器等の端末11-1および端末11-2が接続されている。LAN 1-1と端末11-1および11-2との接続は、例えば、Ethernet（登録商標）（100BASE-TX）等の高速インタフェースによって行われる。端末11-1および11-2は、LAN 1-1およびWAN2を介して、LAN 1-2に接続することができる。

【0032】

LAN 1-2は、LAN 1-1と同様に構成されており、それには、端末11-3が接続されている。

【0033】

各端末11は、著作権で保護される所定のコンテンツを授受できる機器として登録された機器（以下、適宜、このような機器を、正規の機器と称する）である。各端末11は、同一LAN1内にある他の端末11と、このコンテンツを授受することができる。

【0034】

端末11は、図3に示すように、送信可否判定部21、応答制御部22、通信部23、およびコンテンツ格納部24を含んで構成されている。

【0035】

送信可否判定部21は、著作権で保護されたコンテンツ（例えばコンテンツ格納部24に格納されているコンテンツ）を送信する際、受信側の機器との往復伝播時間（RTT: Round Trip Time）に基づいて、受信側の機器が同じLAN1内にあるものか否かを判定するとともに、受信側の機器から正規の機器しか知り得ない情報の提供を受けて、RTT計測の相手と正規の機器しか知り得ない情報の提供者が同一であるか否かを確認する。送信可否判定部21は、この確認結果に基づいて、コンテンツの送信の可否を判定する。

【0036】

図1Cの例では、RTT計測の相手（機器x）と、正規の機器しか知り得ない情報の提供者（受信機器）との同一性を確認しなかったため、送信機器と同一LANに挿入された不正な機器xは、受信機器から、正規の機器しか知り得ない情報を送信機器に供給させることによって、送信機器からコンテンツを不正に入手することができた。しかしながら本発明によれば、後述するようにRTT計測の相手（機器x）と、正規の機器しか知り得ない情報の提供者（受信機器）が同一であることが確認されるので、図1Cに示したような不正は排除される。

【0037】

応答制御部22は、送信側の端末11から所定のコンテンツの提供を受ける際、通信部23を介して、送信側の機器と後述するように通信することで、コンテンツの提供を受けるために必要な情報（RTT計測に必要なデータ、正規の機器しか知り得ない情報、およびRTT計測の相手と正規の機器しか知り得ない情報の提供者が同一であることを確かめるための情報）を送信側の機器に送信する。

【0038】

通信部23は、LAN1に接続されており、同一のLAN1内の機器、またはWAN2を介して異なるLAN1に接続されている機器との通信を行う。

【0039】

コンテンツ格納部24は、受信側の端末11に送信されるコンテンツが格納されている。このコンテンツは、例えば著作権で保護されており、その著作権によりその利用が許可された端末11であって、送信側の端末11と同一LAN1に接続された端末11にのみ提供される。

【0040】

図4は、端末11の送信可否判定部21の構成例を示している。

【0041】

認証データ生成部31は、RTT計測のために受信側の機器に送信される計測コマンドMCを構成する認証データRを生成する。この認証データRは、ランダムチャレンジとして使用されるので、疑似乱数列などの、毎回異なる予測不可能な数列で構成されている。



## 【0042】

計測コマンド送信部32は、認証データ生成部31で生成された認証データRを含む計測コマンドMCを、受信側の機器に送信する。

## 【0043】

計測応答受信部33は、計測コマンド送信部32により送信された計測コマンドMCに対する、受信側の機器からの応答MCRを受信する。

## 【0044】

記憶部34は、計測コマンドMCに挿入された認証データR、および計測コマンドMCに対する受信側の機器からの応答MCRに含まれている応答データSと応答生成時間T（後述）を記憶する。

10

## 【0045】

RTT計測部35は、計測コマンド送信部32および計測応答受信部33からの通知STR、ENDに応じて、受信側の機器との通信往復伝播時間（RTT）を計測する。

## 【0046】

制御コマンド送信部36は、開始コマンドや確認コマンド（後述）の制御コマンドCCを受信側の機器に送信する。制御応答受信部37は、制御コマンドCCに対する受信側の機器からの応答CCRを受信する。

## 【0047】

制御判定部38は、上記各部を制御し、受信側の機器との往復伝播時間（RTT）に基づいて、受信側の機器が同じLAN1内にあるものか否かを判定するとともに、受信側の機器から正規の機器しか知り得ない情報の提供を受けて、RTT計測の相手と正規の機器しか知り得ない情報の提供者が同一であるか否かを確認する。制御判定部38は、この確認結果に基づいて、コンテンツの送信可否を判定する。

20

## 【0048】

なお図4の各部を結ぶ矢印は、主なデータの送受信の流れを表している。

## 【0049】

図5は、端末11の応答制御部22の構成例を示している。

## 【0050】

応答データ生成部52は、計測コマンドMCに対する応答MCRを構成する応答データSを生成する。この応答データSは、ランダムチャレンジとして使用されるので、疑似乱数列など、毎回異なる予測不可能な数値で構成されている。なおここで生成された応答データSと、送信側の機器で生成される認証データRは、それぞれ独立して生成されており、両者が共有するものではない。

30

## 【0051】

計測コマンド受信部53は、送信側の機器からの計測コマンドMCを受信する。

## 【0052】

応答生成時間計測部54は、計測コマンド受信部53からの通知STR、ENDに応じて、計測コマンドMCに対する応答MCRを生成するのに要した時間（以下、応答生成時間と称する）Tを計測する。

## 【0053】

計測応答送信部55は、RTT計測に必要なデータ（応答データSおよび応答生成時間T（後述）等）を含む、計測コマンドMCに対する応答MCRを生成し、送信側の機器に送信する。

40

## 【0054】

記憶部56は、計測コマンドMCに含まれていた認証データR、および応答MCRに含まれて送信された応答データSと応答生成時間Tを記憶する。

## 【0055】

制御コマンド受信部57は、送信側の機器から送信されてきた制御コマンドCCを受信する。制御応答送信部58は、制御コマンドCCに対する応答CCRを送信側の機器に送信する。例えばRTT計測の相手と正規の機器しか知り得ない情報の提供者が同一であることを確

50

認するためのデータが、制御コマンドCCの応答CCRとして送信側の機器に送信される。

【0056】

制御部51は、上記各手段を制御する。

【0057】

次に、送信可否判定処理（端末11の送信可否判定部21の処理）を、図6のフローチャートを参照して説明する。

【0058】

ステップS51において、端末11の送信可否判定部21の制御コマンド送信部36は、受信側の機器と、TCPコネクションを確立する。TCPコネクションのためのポート番号は予め送信側の端末11と受信側の機器の間で合意されているものとする。送信側の機器と受信側の機器の間で事前にTCPコネクションが確立している場合はこのステップを省略してよい。

10

【0059】

制御コマンド送信部36は、確立したTCPコネクションを介して、RTTの計測を開始する旨を表す開始コマンド（制御コマンドCC）を受信側の機器に送信する。この開始コマンドCCには、セッション番号SID、および送信側の端末11が実行可能な、1セッションでのRTTのリトライ数（計測回数） $k_s$ が含まれている。

【0060】

セッション番号SIDは、これから行われる受信側の機器に対する一連の認証処理（1つのセッション）に割り当てられた番号であり、この番号を送信側と受信側とで共有することにより、セッション毎に認証処理を区別することができる。

20

【0061】

またRTT計測のために必要なデータ（例えば、計測コマンドMCやその応答MCR）の通信は、パケットの再送を行わないUDPでなされるので、通信状態によっては、データが途中で消滅してしまうなど、RTT計測が適切に行われない場合も考えられる。またネットワーク内の他の通信の影響を受けて、パケットの伝送に遅延が生じることもある。そこでRTT計測を何回かリトライ（再実行）できるようになされている。このリトライの回数は、送信側の機器と受信側の機器の設定によって異なることもあるので、この例ではここで送信側の機器のリトライ数（例えば、最大のリトライ数） $k_s$ が受信側の機器に通知される。

30

【0062】

次に、ステップS52において、制御応答受信部37は、開始コマンドCCに対する、受信側の機器からの応答CCRを受信する。

【0063】

この応答CCRには、開始コマンドCCに含まれていたセッション番号SIDの他、受信側が決定した1セッションでのRTT計測のリトライ数 $k$ 、および計測コマンドMCを受信するためのUDPポート番号 $p_b$ が含まれている。すなわち開始コマンドCCとその応答CCRにより、送信側の端末11と受信側の機器は、RTT計測のリトライ数（計測回数） $k$ とセッション番号SID、および計測コマンドMCとその応答MCRで利用するUDPポート番号 $p_b$ を合意する。

【0064】

なお受信側の機器は、開始コマンドCCを介して通知された送信側の端末11で実行可能なRTT計測のリトライ数 $k_s$ と受信側が実行可能なRTT計測のリトライ数のうちの小さい方を、RTT計測のリトライ数 $k$ に決定し、応答CCRを介して送信側の機器に通知する。

40

【0065】

ステップS53において、認証データ生成部31は、ステップS52で受信された応答CCRに含まれていたRTT計測のリトライ数 $k$ 分の認証データ（ $k$ 個の認証データ） $R$ を生成する。

【0066】

ステップS54において、制御判定部38に内蔵されるカウンタ $i$ の値が1に初期設定される。このとき認証データ生成部31は、カウンタ $i$ の値に対応する認証データ（例えば、第 $i$ 番目に生成された認証データ $R_i$ ）を、計測コマンド送信部32および記憶部34

50

に供給する。

【0067】

ステップS55において、計測コマンド送信部32は、セッション番号SID、認証データ生成部31から供給された認証データ $R_i$  ( $k$ 個の認証データ $R$ のうちのカウンタ $i$ の値に対応する認証データ $R_i$ )、およびシーケンス番号 $C_i$  (カウンタ $i$ の値を表す番号)を含む計測コマンドMCを、制御コマンドCCの応答CCRに含まれていたUDPポート番号 $p_b$ でのUDP通信で、受信側の機器に送信する。

【0068】

計測コマンド送信部32は、計測コマンドMCを送信したとき、その旨の通知STRをRTT計測部35に行う。これによりRTT計測部35は、RTTの計測を開始する。

10

【0069】

記憶部34は、認証データ生成部31から供給された認証データ $R_i$ を、カウンタ $i$ の値に対応させて(シーケンス番号 $C_i$ に対応させて)記憶する。

【0070】

ステップS56において、計測応答受信部33は、受信側の機器からの応答MCRを受信したか否かを判定し、受信していないと判定した場合、ステップS57に進み、所定時間以上応答を待っているか否かを判定する(ステップS55でRTT計測が開始されてから所定の時間経過したか否かを判定する)。

【0071】

ステップS57で、まだ所定の時間していないと判定された場合、ステップS56に戻り、それ以降の処理が実行される。一方ステップS57で所定の時間経過したと判定された場合、ステップS62に進み、カウンタ $i$ の値がリトライ数 $k$ より大きいか否かが判定され(RTT計測が $k$ 回行われたか否かが判定され)、まだ大きくないと判定された場合( $k$ 回行われていない場合)、ステップS63に進み、カウンタ $i$ の値を1だけインクリメントされて、ステップS55に戻る。

20

【0072】

計測コマンドMCを送るUDPでは、パケットが通信相手に届かないことがあるので、送信側の端末11は、計測コマンドMCを送った後、所定時間が経っても応答MCRが受信されない場合は、この回の計測は失敗したものとして、次のRTT計測が開始される(ステップS55に戻る)。

30

【0073】

ステップS56で、応答MCRが受信されたと判定された場合、ステップS58に進み、計測応答受信部33は、受信した応答MCRに含まれている応答データ $S_j$ 、シーケンス番号 $C_j$ 、および応答生成時間 $T_j$ を読み出し、制御判定部38に供給する。

【0074】

制御判定部38は、計測応答受信部33から供給されたシーケンス番号 $C_j$ が、カウンタ $i$ の値(送信された計測コマンドMCのシーケンス番号 $C_i$ )と一致するか否かを判定する。なお応答MCRのシーケンス番号 $C_j$ と計測コマンドMCのシーケンス番号 $C_i$ を確認する意味については後述する。

【0075】

ステップS58において、一致しないと判定された場合、ステップS56に戻り、それ以降の処理が行われ、一致すると判定された場合、ステップS59に進む。

40

【0076】

ステップS59において、計測応答受信部33は、応答MCRを受信した旨の通知ENDをRTT計測部35に行う。RTT計測部35は、ステップS55で開始したRTT計測を終了し、計測結果(RTT)を、制御判定部38に供給する。

【0077】

ステップS60において、計測応答受信部33は、受信した応答MCRに含まれていた応答データ $S_j$ および応答生成時間 $T_j$ を、記憶部34に供給する。記憶部34は、カウンタ $i$ の値に対応させて、計測応答受信部33から供給された応答データ $S_j$ と応答生成時間 $T_j$ を

50

記憶する。すなわち記憶部34には、カウンタ $i$ の値に対応して、認証データ $R_i$ （ステップS55）、応答データ $S_j$ 、および応答生成時間 $T_j$ が記憶される。

【0078】

なお応答生成時間 $T$ とは、詳細は後述するが、受信側の機器で、計測コマンド $MC$ に対する応答 $MCR$ を生成するのに要した時間である。

【0079】

ステップS61において、制御判定部38は、RTT計測部35から供給されたRTTから、計測応答受信部33から供給された応答生成時間 $T_j$ （応答 $MCR$ に含まれていた応答生成時間 $T_j$ ）を減算し、その減算結果得られた値が、所定の規定時間 $TL$ より大きいかな否かを判定する。

【0080】

ここで計測されたRTTは、計測コマンド $MC$ の受信側の機器への伝送時間、受信側での応答 $MCR$ を生成するのに要した応答生成時間 $T$ 、そして応答 $MCR$ の送信側の端末11への伝送時間の合計となるので、そこから応答 $MCR$ を生成するのに要した応答生成時間 $T$ を減算することで、実質的な往復伝播時間を求めることができる。

【0081】

規定時間 $TL$ は、実質的な往復伝播時間が、送信側の端末11と受信側の機器が同一LAN1に接続されていたならば、それを超えないであろう時間である。すなわち実質的な往復伝播時間が規定時間 $TL$ より大きければ、受信側の機器は送信側の端末11と同一のLAN1に接続されていないと判定することができる。一方、実質的な往復伝播時間が規定時間 $TL$ より大きくない（それ以下である場合）、受信側の機器は送信側の端末11と同一LAN1に接続されていると判定することができる。

【0082】

ステップS61で、YESの判定がなされたとき（第 $i$ 回目のRTT計測で、受信側の機器が送信側の端末11と同一のLAN1に接続されているものではないと判定されたとき）、ステップS62に進み、制御判定部38は、カウンタ $i$ の値が $k$ より大きい値かな否か（RTT計測が $k$ 回リトライされたかな否か）を判定し、大きくないと判定した場合（RTT計測がまだ $k$ 回行われていない場合）、ステップS63に進み、カウンタ $i$ の値が1だけインクリメントされる。このとき認証データ生成部31は、カウンタ $i$ の新たな値に対応する認証データ $R_i$ を、計測コマンド送信部32および記憶部34に供給する。

【0083】

その後ステップS55に戻り、それ以降の処理が行われる。すなわち実質的な往復伝播時間が規定時間 $TL$ 内になる応答 $MCR$ が得られないときは、最大 $k$ 回、RTT計測が行われる。

【0084】

ステップS61で、NOの判定がなされたとき（実質的な往復伝播時間が規定時間 $TL$ 以下となる応答 $MCR$ が得られたとき）、ステップS64に進む。

【0085】

ステップS64において、制御コマンド送信部36は、このセッションで最後に受信した計測コマンド $MC$ に含まれていた認証データ $R$ と、その計測コマンド $MC$ に対する応答 $MCR$ に含まれていた応答データ $S$ と応答生成時間 $T$ の送信を要求する制御コマンド（確認コマンド） $CC$ を、受信側の機器に送信する。

【0086】

ステップS65において、制御応答受信部37は、受信側の機器から送信されてきた、ステップS64で送信された確認コマンド $CC$ に対する応答 $CCR$ を受信すると、それを制御判定部38に供給する。

【0087】

応答 $CCR$ には、例えば受信側の機器が最後に受信した計測コマンド $MC$ に含まれている認証データ $R$ と、その計測コマンド $MC$ に対する応答 $MCR$ に含まれていた応答データ $S$ と応答生成時間 $T$ に対して、正規の機器が共有する秘密鍵に基づくハッシュ処理が施されたハッシュ値（署名）が示されている。

10

20

30

40

50

## 【0088】

ステップS66において、制御判定部38は、制御応答受信部37から供給された応答CCRに基づいて、受信側の機器にコンテンツを送信できるか否かを判定する。

## 【0089】

具体的には制御判定部38は、最後に受信側の機器に送信した計測コマンドMCに含まれていた認証データRと、その計測コマンドMCに対する応答MCRに含まれていた応答データSと応答生成時間Tを記憶部34から読み出すとともに、正規の機器が共有する秘密鍵に基づくハッシュ処理を施す。

## 【0090】

そして制御判定部38は、応答CCRに示されるハッシュ値と、ここでのハッシュ処理の結果得られたハッシュ値が一致するか否かを判定し、一致すると判定した場合、RTT計測相手と、正規の機器のみが知り得る情報（署名）の提供者とが一致すると判定し、コンテンツを受信側の機器に送信できると判定する。RTT計測相手と正規の機器のみが知り得る情報の提供者とが一致することを確認するための認証データR、応答データS、および応答処理時間Tを、適宜、確認データQと称する。

## 【0091】

また応答CCRに示される署名が、確認データQの全部または一部が著作権保護のための秘密鍵で暗号化されて生成されている場合、制御判定部38は、その公開鍵でその署名を復号し、その結果得られた確認データQと、記憶部34から読み出した確認データQが一致するか否かを判定する。

## 【0092】

ステップS66で、コンテンツを受信側の機器（端末11）に送信できると判定された場合（RTT計測の相手と、正規の機器しか知り得ない情報の提供者が一致した場合）、ステップS67に進み、制御判定部38は、受信側の機器は、コンテンツを送信できる機器（コンテンツを利用できる機器であって、送信側の端末11と同じLAN1に接続されている機器）である旨を、通信部23（図3）に通知する。これにより通信部23は、所定のコンテンツをコンテンツ格納部24から読み出して、受信側の機器（端末11）に送信する。

## 【0093】

ステップS66で、コンテンツを受信側の機器に送信できないと判定された場合（RTT計測の相手であった相手と、正規の機器しか知り得ない情報の提供者が一致しない場合）、ステップS68に進み、制御判定部38は、受信側の機器は、不正な機器であるとして、コンテンツを送信することができない旨を、通信部23に通知する。これにより通信部23は、コンテンツの受信側の機器への送信を行わない。

## 【0094】

ステップS62で、カウンタiの値が、kより大きいと判定された場合（RTT計測をk回行っても、実質的な往復伝播時間が規定時間TL以下になる応答MCRが得られなかった場合）、ステップS69に進み、制御判定部38は、受信側の機器は、ローカルネットワーク外の機器（同じLAN1に接続されていない機器）である旨を、通信部24に通知する。これにより通信部23は、コンテンツの受信側の機器への送信を行わない。

## 【0095】

ステップS70において、制御コマンド送信部36は、終了コマンド（制御コマンド）CCを受信側の機器に送信する。

## 【0096】

以上のようにして送信可否判定処理が行われる。

## 【0097】

以上の説明では、ステップS52においてk個の認証データRを生成したが、それに代えて、ステップS55において、計測コマンドMCを送信する毎にそのコマンドに使う認証データRを毎回生成するようにしてもよい。

## 【0098】

10

20

30

40

50

次に、応答制御処理（端末 11 の応答制御部 22 の処理）を、図 7 のフローチャートを参照して説明する。

【0099】

ステップ S 81 において、端末 11 の応答制御部 22 の制御コマンド受信部 57 は、送信側の機器と協働して、TCPコネクションを確立し、そのTCPコネクションを介して送信側の機器から送信されてきた、RTT計測の開始する旨を表す開始コマンド CC（ステップ S 51）を受信する。

【0100】

次にステップ S 82 において、計測コマンド受信部 53 は、送信側の機器から送信されてくる計測コマンド MCを受信するためのUDPポート番号 p b を決定する。

10

【0101】

計測コマンド受信部 53 はまた、制御コマンド CCに含まれている送信側の機器が実行可能なRTTのリトライ数 ks と、受信側の端末 11 が対応可能なRTT計測のリトライ数のいずれか小さい方を、今回のRTT計測のリトライ数 k に決定する。そして応答データ生成部 52 は、k 個の応答データ S を生成する。

【0102】

ステップ S 83 において、制御応答送信部 58 は、ステップ S 81 で受信された制御コマンド CCに含まれていたセッション番号 SID、RTT計測のリトライ数 k、およびUDPポート番号 p b を含む応答 CCR を、ステップ S 81 で確立されたTCPコネクトを介して送信側の機器に送信する。送信側の機器は、ここで送信された応答 CCRを受信する（ステップ S 52）

20

【0103】

ステップ S 84 において、制御部 51 に内蔵されているカウンタ j の値が 0 に初期設定される。

【0104】

ステップ S 85 において、コマンドが受信されたか否かが判定され、コマンドが受信されたと判定された場合、ステップ S 86 に進み、受信されたコマンドが計測コマンド MC（ステップ S 55）であるか否かを判定し、計測コマンド MCであると判定された場合、ステップ S 87 に進む。

30

【0105】

ステップ S 87 において、計測コマンド受信部 53 は、計測コマンド MCに含まれているシーケンス番号 Ci がカウンタ j の値より大きいと判定し、シーケンス番号 Ci がカウンタ j の値より大きいと判定した場合、ステップ S 88 に進む。なおここでの処理の意味については、図 6 のステップ S 58 の処理を合わせて後述する。

【0106】

ステップ S 88 において、計測コマンド受信部 53 は、計測コマンド MCが受信された旨の通知 STR を応答生成時間計測部 54 に行う。これにより応答生成時間計測部 54 は、応答生成時間の計測を開始する。

【0107】

ステップ S 89 において、カウンタ j の値が計測コマンド MCに含まれているシーケンス番号 Ci の値に設定される。このとき応答データ生成部 52 は、設定されたカウンタ j の値に対する応答データ Sj を、計測応答送信部 55 および記憶部 56 に供給する。

40

【0108】

次にステップ S 90 において、計測コマンド受信部 53 は、受信した計測コマンド MCに含まれている認証データ Ri を読み出し、記憶部 56 および計測応答送信部 55 に供給する。記憶部 56 は、計測コマンド受信部 53 から供給された認証データ Ri を、カウンタ j の値に対応させて記憶する。

【0109】

ステップ S 91 において、計測コマンド受信部 53 は、認証データ Ri の読み出しが完了した旨の通知 END を応答生成時間計測部 54 に行う。これにより応答生成時間計測部 55

50

は、ステップS88で開始した応答生成時間計測を終了し、計測結果Tjを計測応答送信部55および記憶部56に供給する。

【0110】

ステップS92において、計測応答送信部55は、セッション番号SID、カウンタjの値を表すシーケンス番号Cj、応答データ生成部52から供給された応答データSj、および応答生成時間計測部54から供給された応答生成時間Tjを含む応答MCRを、送信側の機器に送信する。記憶部56は、応答データSjおよび応答生成時間Tjを、カウンタjの値に対応させて記憶する。すなわち記憶部56には、認証データRi（ステップS90）、応答データSjおよび応答生成時間Tjが、カウンタjの値に対応して記憶されている。

【0111】

ステップS86で、計測コマンドMCではないと判定された場合、ステップS93に進み、確認コマンドCC（S64）が受信されたか否かが判定され、確認コマンドCCが受信されたと判定した場合、ステップS94に進む。

【0112】

ステップS94において、制御応答送信部58は、記憶部56から、最後に受信された計測コマンドMCに含まれていた認証データRi、その計測コマンドMCに対する応答MCRに含まれていた応答データSjと応答生成時間Tjを、署名を付して、送信側の機器に送信する。

【0113】

ステップS93で、確認コマンドCCではないと判定された場合（終了コマンドCC（ステップS70）が受信された場合）、処理は終了する。

【0114】

以上のようにして、応答制御処理が実行される。

【0115】

以上の説明では、ステップS82において最初にk個の応答データSを生成したが、それに代えて、ステップS90において、計測コマンドMCを受信する毎にそのコマンドに対する応答MCRで使う応答データSを生成するようにしてもよい。あるいは、ステップS82においては最初に1個の応答データS1を生成し、ステップS92において応答MCRを送信した後に、次のコマンドMCに対する応答MCRの応答データSを生成するようにしてもよい。

【0116】

次に図6のステップS58の処理の意味について説明する。ステップS58の処理では、受信側の機器からの応答MCRのシーケンス番号Cjと計測コマンドMCのシーケンス番号Ci（カウンタiの値）が一致するか否かが判定されるが、このように計測コマンドMCと応答MCRの対応関係を確認するようにしたので、計測コマンドMCに対応しない応答MCR（他の計測コマンドMCの応答MCR）に基づいてRTT認証が行われないようにすることができる。

【0117】

例えば、図8に示すように、受信側の機器で、第1番目の計測コマンドMCに対する応答MCRの送信に時間がかかり（ステップS92）、送信側の端末11で、タイムアウトと判定されて（ステップS57）、第2番目の計測コマンドMCが受信側の機器に送信されたものとする。第1番目の計測コマンドMCに対する応答MCRは、第2番目の計測コマンドMCが送信された後（ステップS55）、第2番目の計測コマンドMCとの関係ではタイムアウトとならない間（ステップS57）に送信側の端末11に受信されたものとする（ステップS56）。

【0118】

しかしながら本発明では、受信側の機器からの応答MCRのシーケンス番号（=1）と、第2番目の計測コマンドMCのシーケンス番号（=2）が一致しないと判定され、送信側の端末11は、第2番目の計測コマンドMCに対する応答MCRが受信されるまで待機することになり（ステップS56に戻る）、対応しない応答MCRが受信されてもRTT認証は行われない。

【0119】

次に図7のステップS87の処理の意味を説明する。例えば図9に示すように、第1番

10

20

30

40

50

目の計測コマンドMCでのRTT計測で、規則時間TL内の応答MCRが得られず、第2番目の計測コマンドMCが送信される場合において、第2番目の計測コマンドMCの受信側の端末11への到着が遅れ、第2番目の計測コマンドMCについてもタイムアウトと判定されて、送信側の機器からは第3番目の計測コマンドMCが受信側の端末11へ送信されたとする。

【0120】

第2番目の計測コマンドMCは、第3番目の計測コマンドMCの受信の後、そしてその計測コマンドMCに対する応答MCRの送信の後、受信側の端末11に到着したものとする。

【0121】

受信側の端末11では、第2番目の計測コマンドMCの応答MCRを生成するとき、カウンタjの値は3になっているので（すでに第3番目の計測コマンドMCの応答MCRを生成しているので）、第2番目の計測コマンドMCに対する応答MCRを生成する際、第2番目の計測コマンドMCのシーケンス番号（=2）<カウンタj（=3）であることからステップS87でNOの判定がなされ、第2番目の計測コマンドMCに対する応答MCRは生成されない。

10

【0122】

すなわちステップS87の処理により、計測コマンドMCに対応しない応答MCRに基づいてRTTの認証が行われないようになされている。

【0123】

次に、不正に対する端末11の動作を具体的に説明する。

【0124】

例えば図1Cに示した、送信側の端末11と同一のLAN1に接続された不正な機器xに対して、送信可否判定処理が開始されると、ステップS51乃至ステップS55の処理で、送信側の端末11からは、図10に示すように、第1番目の計測コマンドMCが不正機器xに送信される。

20

【0125】

不正機器xからは、応答制御処理におけるステップS81乃至S92の処理により、第1番目の計測コマンドMCの応答MCRが送信側の端末11に送信される。

【0126】

この例の場合、不正機器xは、送信側の端末11と同一のLAN1に接続されているので、RTT計測の結果、同一LAN1に接続されている機器と判定され（ステップS61でNOの判定がなされ）、ステップS64、S65の処理により、送信側の端末11から不正機器xへ確認コマンドCCが送信される。

30

【0127】

不正機器xは、第1番目の計測コマンドMCの応答MCRを送信した後、確認コマンドCCを受信すると、ステップS94の処理により、最後の計測コマンドMCに含まれた認証データ（第1番目の計測コマンドMCの認証データR1）、その計測コマンドMCの応答MCRに含まれていた応答データS1と応答生成時間T1を送信側の端末11に送信しようとする。しかしながら、不正機器xは、適切な署名を生成する情報を有していないので、例えば署名なしで若しくは不適当な署名を付してこれらのデータを応答CCRとして送信側の端末11に送信する。

【0128】

送信側の端末11はこの場合、署名の照合をすることができないので、RTT計測相手と正規の機器のみが知りうる情報の提供者が一致しないと判定し（ステップS66）、コンテンツの送信は行われない（ステップS68）。

40

【0129】

また計測コマンドMCに対する応答MCRは、送信側の端末11と同じLAN1に接続されている不正機器xが行い、確認コマンドCCに対する応答CCRは正規の端末11によって行われるようにする不正も考えられる。

【0130】

この場合不正機器xは、はじめに送信側の端末11になりすまし、ステップS51乃至ステップS55の処理で、認証データRaを含む計測コマンドMCを受信側の端末11に送信

50



し、受信側の端末 11 から、ステップ S 81 乃至ステップ S 92 の処理で、応答データ Sa と応答生成時間 Ta を含む応答 MCR を送信させて取得する。

#### 【0131】

そしてその後は、不正機器 x は、受信側の端末 11 になりすまし、送信側の端末 11 によるステップ S 51 乃至ステップ S 55 の処理により、送信側の端末 11 から送信されてきた、認証データ Rb を含む計測コマンド MC を受信すると、先に正規の受信側の端末 11 から取得しておいた応答 MCR に含まれる応答データ Sa と、ステップ S 61 で NO の判定されるのに十分大きな応答生成時間 Ta' を含む応答 MCR を送信側の端末 11 に送信する（ステップ S 92）。

#### 【0132】

その結果送信側の端末 11 からは確認コマンド CC が送信されてくるので（ステップ S 64）、不正機器 x はそれをそのまま受信側の端末 11 に送信する。確認コマンド CC を受信した受信側の端末 11 は、最後に受信した計測コマンド MC に含まれる認証データ（いまの例の場合、不正機器 x からの計測コマンド MC に含まれていた認証データ Ra）と、その計測コマンド MC に対する応答 MCR に含まれていた応答データ Sa と応答生成時間 Ta に署名を付して、応答 CCR として送信側の端末 11 に送信する。

#### 【0133】

送信側の端末 11 では、受信側の端末 11 からの応答 CCR の署名を解読することはできるが、この応答 CCR に含まれる認証データ Ra が、送信側の端末 11 が最後に送信した認証データ（不正機器 x に送信した計測コマンド MC の認証データ Rb）と一致しないので（ステップ S 66 で NO の判定がなされるので）、不正機器 x へのコンテンツ提供を行われない。

#### 【0134】

このようにして本発明によれば、不正を適切に排除することができる。

#### 【0135】

なお以上においては、受信側の端末 11 において、応答生成時間を、応答 MCR を生成する毎に計測したが、例えば最低必要な時間などの所定の時間に予め決めておき、その時間（固定値）を応答生成時間 T とすることもできる。

#### 【0136】

また応答生成時間 T が通信往復伝播時間の計測に影響がないほどの大きさである場合（通信伝播時間が長い場合または受信側の機器の実装において、応答生成処理が十分に短い時間で行われる場合）は、応答生成時間 T を考慮する必要はない。

#### 【図面の簡単な説明】

#### 【0137】

【図 1】従来の通信システムの利用例を示す図である。

【図 2】本発明を適用した通信システムの利用例を示す図である。

【図 3】図 2 の端末の構成例を示すブロック図である。

【図 4】図 3 の送信可否判定部の構成例を示すブロック図である。

【図 5】図 3 の応答制御部の構成例を示すブロック図である。

【図 6】送信可否判定処理を説明するフローチャートである。

【図 7】応答制御処理を説明するフローチャートである。

【図 8】図 2 の端末の動作を説明する図である。

【図 9】図 2 の端末の動作を説明する他の図である。

【図 10】図 2 の端末の動作を説明する他の図である。

【図 11】図 2 の端末の動作を説明する他の図である。

#### 【符号の説明】

#### 【0138】

11 端末、 21 送信可否判定部、 22 応答制御部、 23 通信部、 24 コンテンツ格納部、 31 認証データ生成部、 32 計測コマンド送信部、 33 計測応答受信部、 34 記憶部、 35 RTT 計測部、 36 制御コマンド送信部、 37 制御応答受信部、 38 制御判定部、 51 制御部、 52 応答データ

10

20

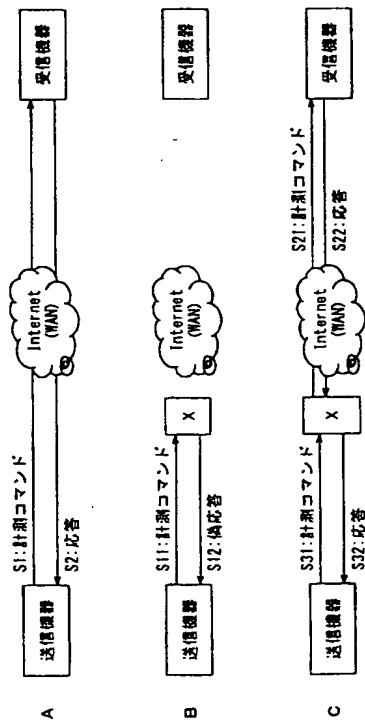
30

40

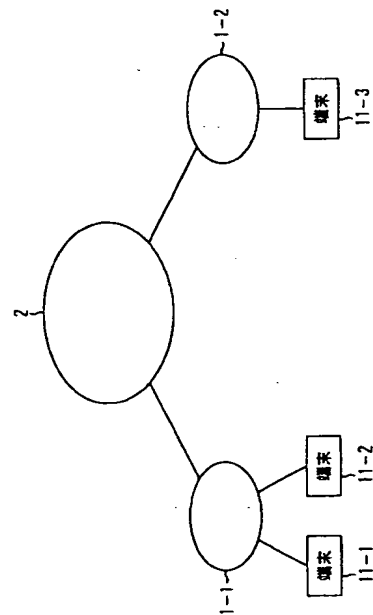
50

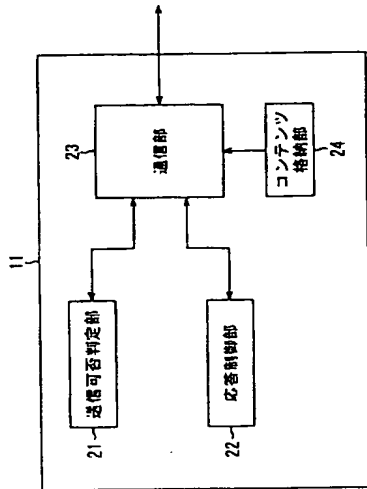
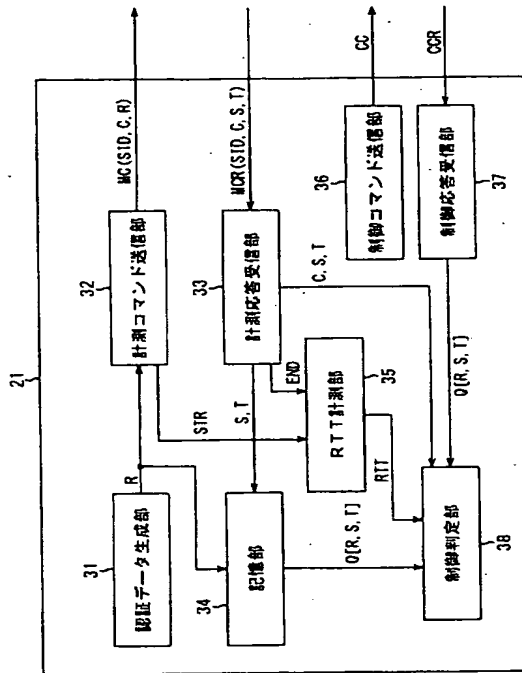
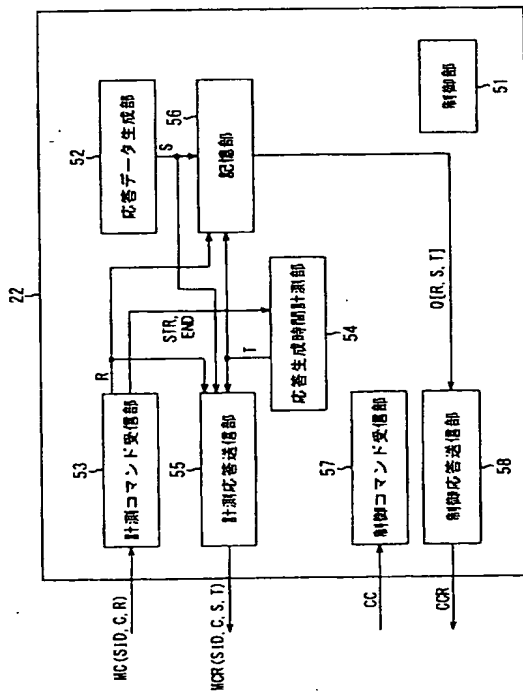
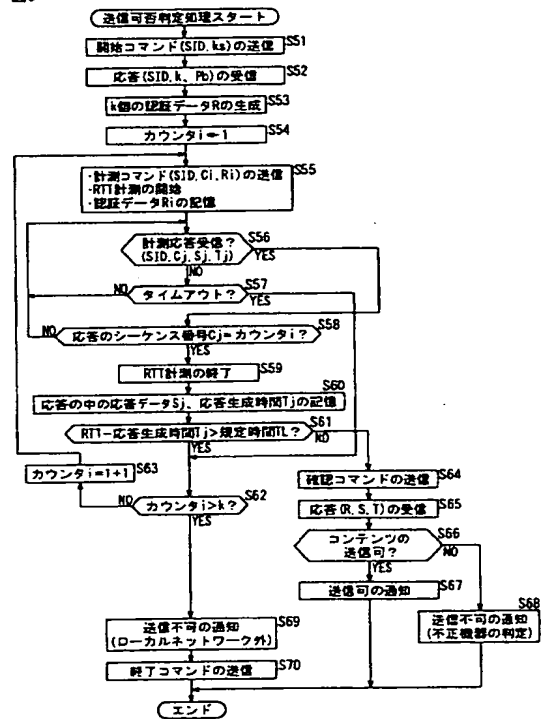
生成部, 53 計測コマンド受信部, 54 応答生成時間計測部, 55 計測応答  
送信部, 56 記憶部, 57 制御コマンド受信部, 58 制御応答送信部

【図1】  
図1

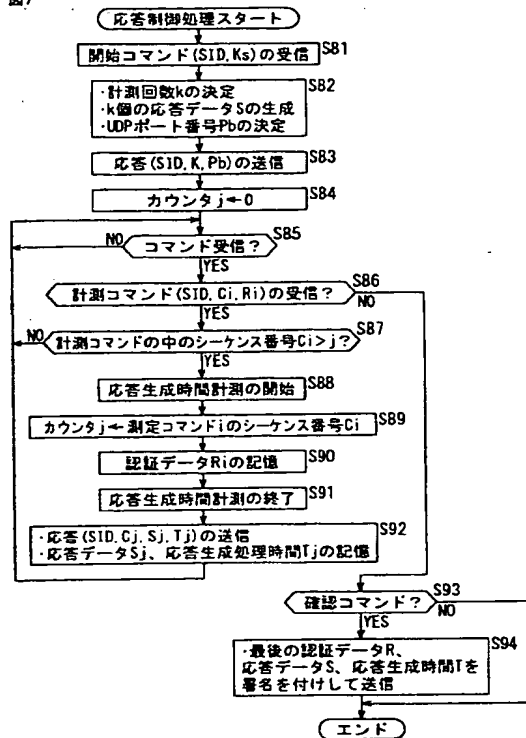


【図2】  
図2

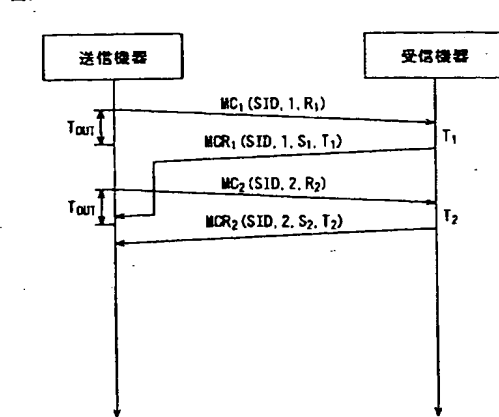


【図 3】  
図3【図 4】  
図4【図 5】  
図5【図 6】  
図6

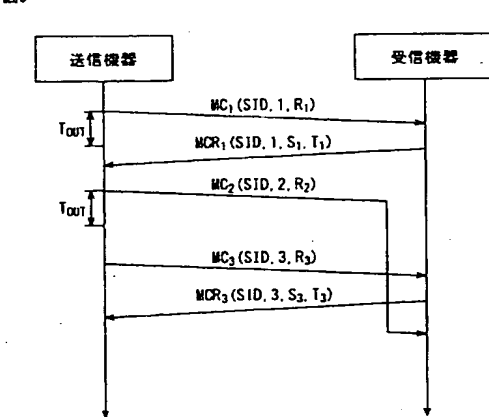
【図 7】



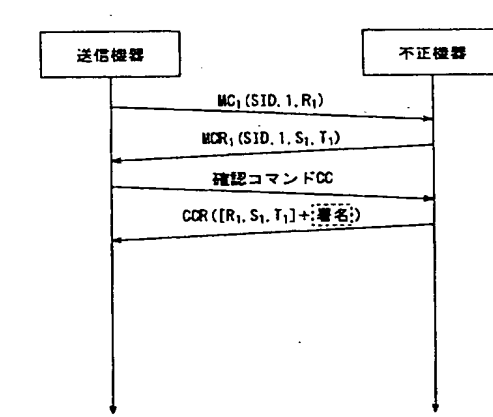
【図 8】



【図 9】

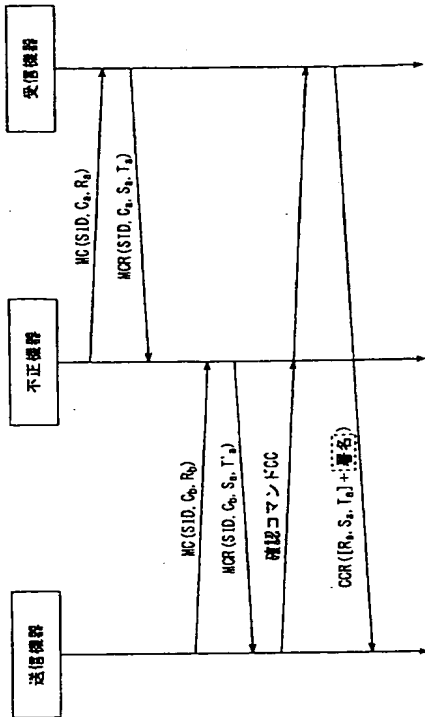


【図 10】



【図 11】

図11



## 【手続補正書】

【提出日】平成17年7月15日(2005.7.15)

## 【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】0042

【補正方法】変更

## 【補正の内容】

【0042】

計測コマンド送信部32は、認証データ生成部31で生成された認証データRを含む計測コマンドMCを、受信側の機器にUDP通信で送信する。

## 【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0046

【補正方法】変更

## 【補正の内容】

【0046】

制御コマンド送信部36は、開始コマンドや確認コマンド(後述)の制御コマンドCCを受信側の機器にICP通信で送信する。制御応答受信部37は、制御コマンドCCに対する受信側の機器からの応答CCRを受信する。

## 【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0053

【補正方法】変更

## 【補正の内容】

【0053】

計測応答送信部 55 は、RTT 計測に必要なデータ（応答データ S および応答生成時間 T（後述）等）を含む、計測コマンド MC に対する応答 MCR を生成し、送信側の機器に UDP 通信 で送信する。

【手続補正 4】

【補正対象書類名】明細書

【補正対象項目名】0055

【補正方法】変更

【補正の内容】

【0055】

制御コマンド受信部 57 は、送信側の機器から送信されてきた制御コマンド CC を受信する。制御応答送信部 58 は、制御コマンド CC に対する応答 CCR を送信側の機器に TCP 通信 で送信する。例えば RTT 計測の相手と正規の機器しか知り得ない情報の提供者が同一であることを確認するためのデータが、制御コマンド CC の応答 CCR として送信側の機器に送信される。

【手続補正 5】

【補正対象書類名】明細書

【補正対象項目名】0058

【補正方法】変更

【補正の内容】

【0058】

まず始めに、端末 11 の送信可否判定部 21 の制御コマンド送信部 36 は、受信側の機器と、TCP 接続を確立する。TCP 接続のためのポート番号は予め送信側の端末 11 と受信側の機器の間で合意されているものとする。送信側の機器と受信側の機器の間で事前に TCP 接続が確立している場合はこのステップを省略してよい。

【手続補正 6】

【補正対象書類名】明細書

【補正対象項目名】0059

【補正方法】変更

【補正の内容】

【0059】

次に、ステップ S51 において、制御コマンド送信部 36 は、確立した TCP 接続を介して、RTT の計測を開始する旨を表す開始コマンド（制御コマンド CC）を受信側の機器に送信する。この開始コマンド CC には、セッション番号 SID、および送信側の端末 11 が実行可能な、1 セッションでの RTT のリトライ数（計測回数） $k_s$  が含まれている。

【手続補正 7】

【補正対象書類名】明細書

【補正対象項目名】0071

【補正方法】変更

【補正の内容】

【0071】

ステップ S57 で、まだ所定の時間が経過していないと判定された場合、ステップ S56 に戻り、それ以降の処理が実行される。一方ステップ S57 で所定の時間経過したと判定された場合、ステップ S62 に進み、カウンタ  $i$  の値がリトライ数  $k$  より大きいか否かが判定され（RTT 計測が  $k$  回行われたか否かが判定され）、まだ大きくないと判定された場合（ $k$  回行われていない場合）、ステップ S63 に進み、カウンタ  $i$  の値を 1 だけインクリメントされて、ステップ S55 に戻る。

【手続補正 8】

【補正対象書類名】明細書

【補正対象項目名】0090

【補正方法】変更

## 【補正の内容】

## 【0090】

そして制御判定部38は、応答CCRに示されるハッシュ値と、ここでのハッシュ処理の結果得られたハッシュ値が一致するか否かを判定し、一致すると判定した場合、RTT計測相手と、正規の機器のみが知り得る情報（署名）の提供者とが一致すると判定し、コンテンツを受信側の機器に送信できると判定する。RTT計測相手と正規の機器のみが知り得る情報の提供者とが一致することを確認するための認証データR、応答データS、および応答生成時間Tを、適宜、確認データQと称する。

## 【手続補正9】

【補正対象書類名】明細書

【補正対象項目名】0109

【補正方法】変更

## 【補正の内容】

## 【0109】

ステップS91において、計測コマンド受信部53は、認証データR<sub>i</sub>の読み出しが完了した旨の通知ENDを応答生成時間計測部54に行う。これにより応答生成時間計測部54は、ステップS88で開始した応答生成時間計測を終了し、計測結果T<sub>j</sub>を計測応答送信部55および記憶部56に供給する。

## 【手続補正10】

【補正対象書類名】図面

【補正対象項目名】図7

【補正方法】変更

## 【補正の内容】

【図7】

図7

